

Fig. 1

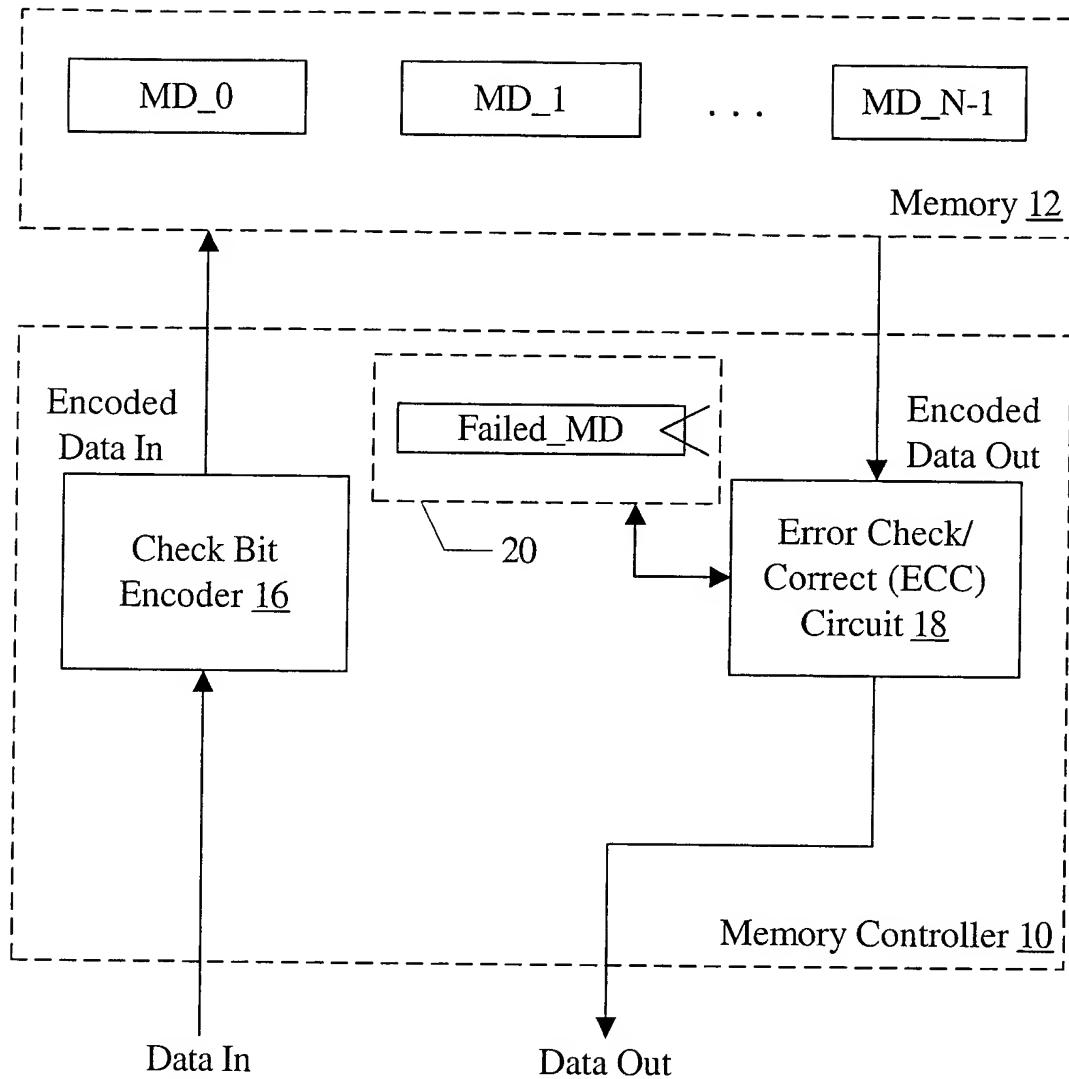


Fig. 2

	c_0	c_1	\dots	\dots	c_{N-1}
r_0					
r_1					
\vdots					
r_{R-1}					
	M	M			M
	D	D			D
	$\bar{0}$	$\bar{1}$			\bar{N}
					-1

Fig. 3

	c_0	c_1	c_{N-1}
r_0			
r_1	R	I	
	o	n	
	w	e	
:		r	
	C	C	
	h	h	
	e	e	
	c	c	
	k	k	
	B	B	
	i	i	
	t	t	
	s	s	
r_{R-1}			
			Data

Fig. 4

Check_Vector(r_x, c_y) = $\text{key}_y * \alpha^x$ (in $\text{GF}(2^R)$) $\leftarrow 30$

row_syn * key_i = inner_syn (in $\text{GF}(2^R)$) $\leftarrow 32$

Check_Vector(r_1, c_1) XOR Check_Vector(r_2, c_2) XOR
Check_Vector(r_1, c_3) XOR Check_Vector(r_2, c_3) $\neq 0$ $\leftarrow 34$
for any r_1, r_2, c_1, c_2, c_3 such that $((r_1, c_1) \neq (r_2, c_2))$ and $c_1 \neq c_3$ or $(c_1 \neq c_2)$

$\text{key}_i + \text{key}_j \neq (\text{key}_i + \text{key}_k) * \alpha^x$ $0 \leq x \leq R-1, i \neq k, i \neq j, j \neq k$ $\leftarrow 36$

Fig. 5

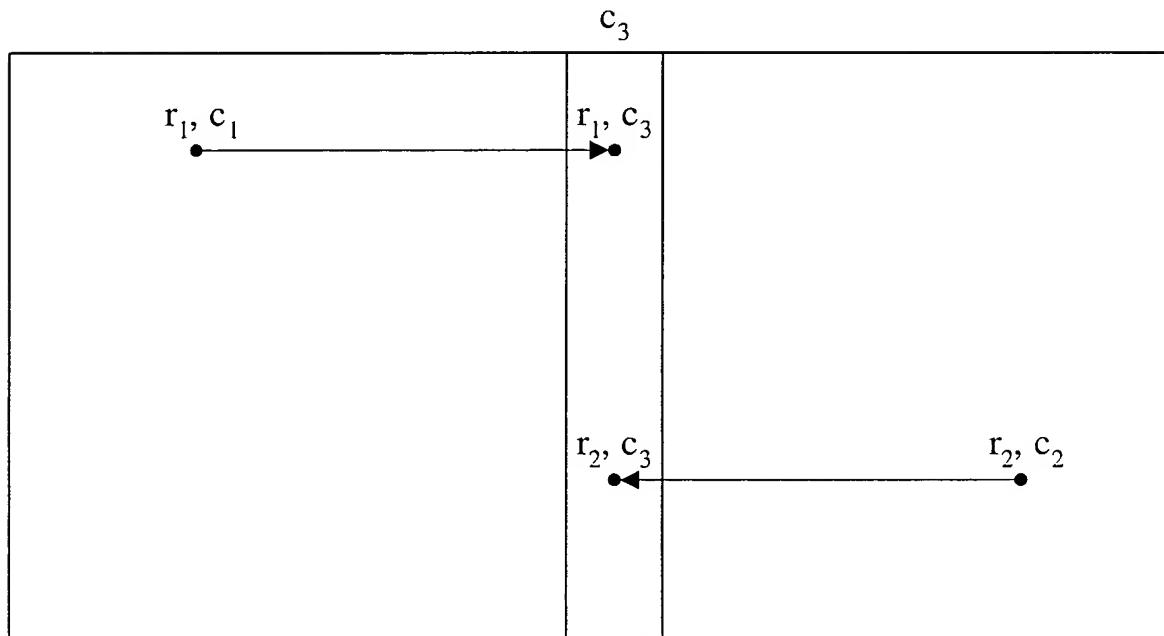


Fig. 6

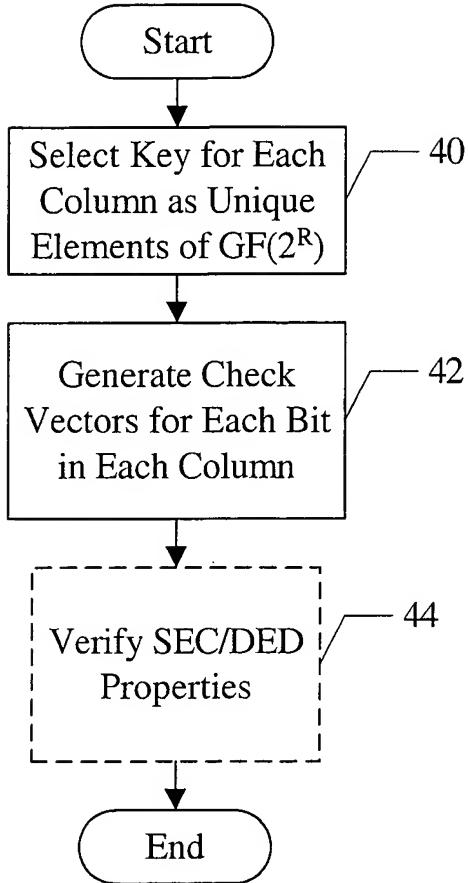


Fig. 7

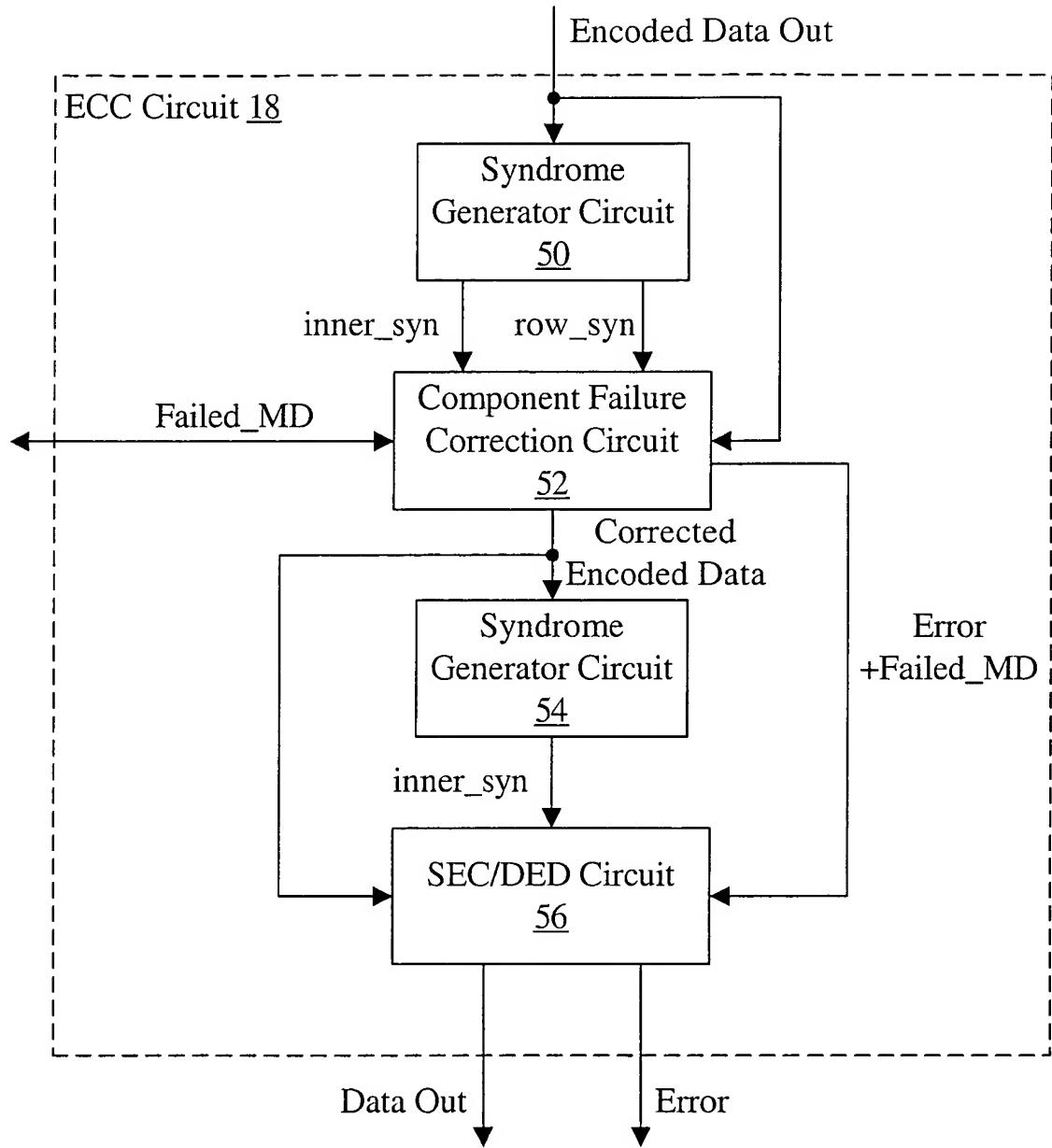


Fig. 8

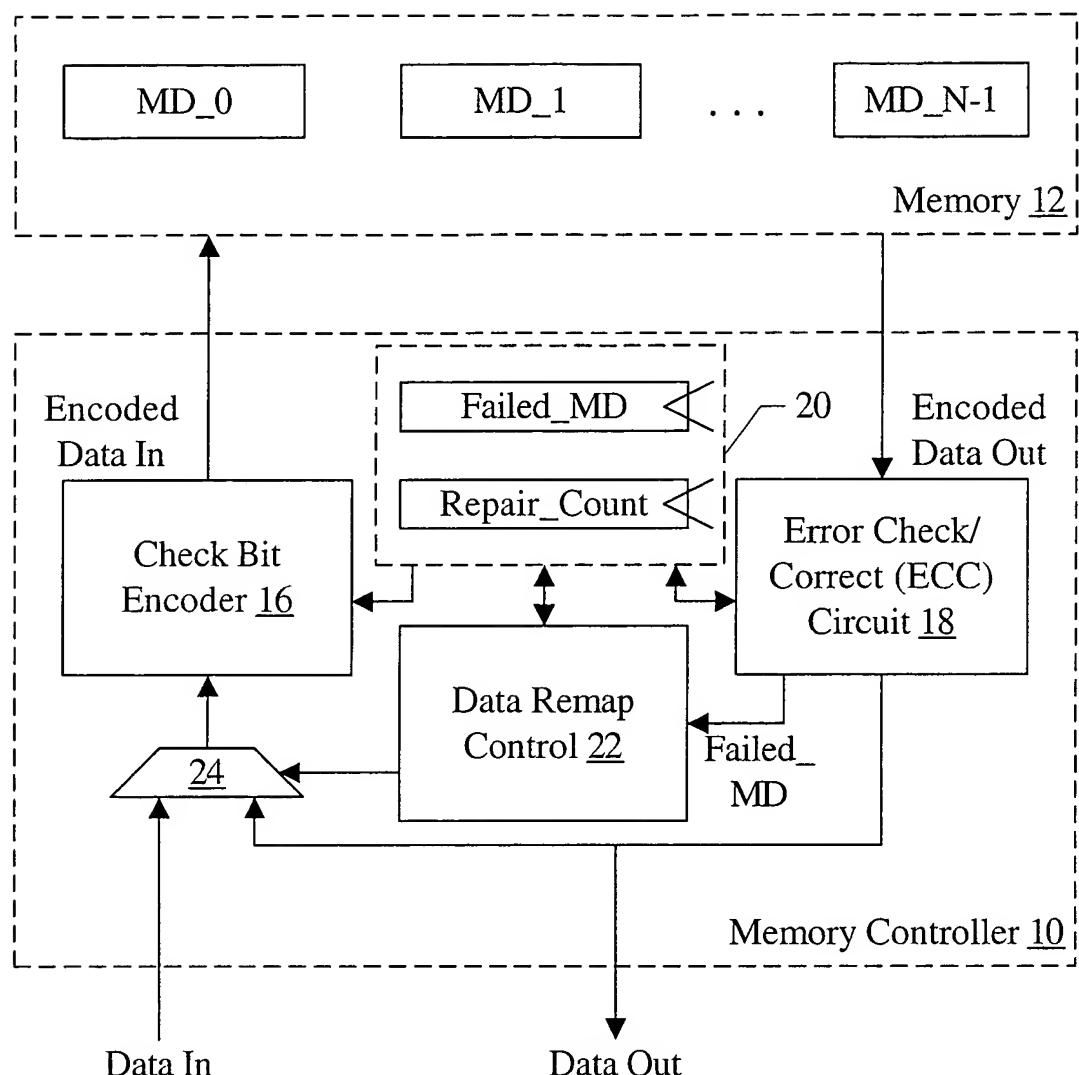


Fig. 9

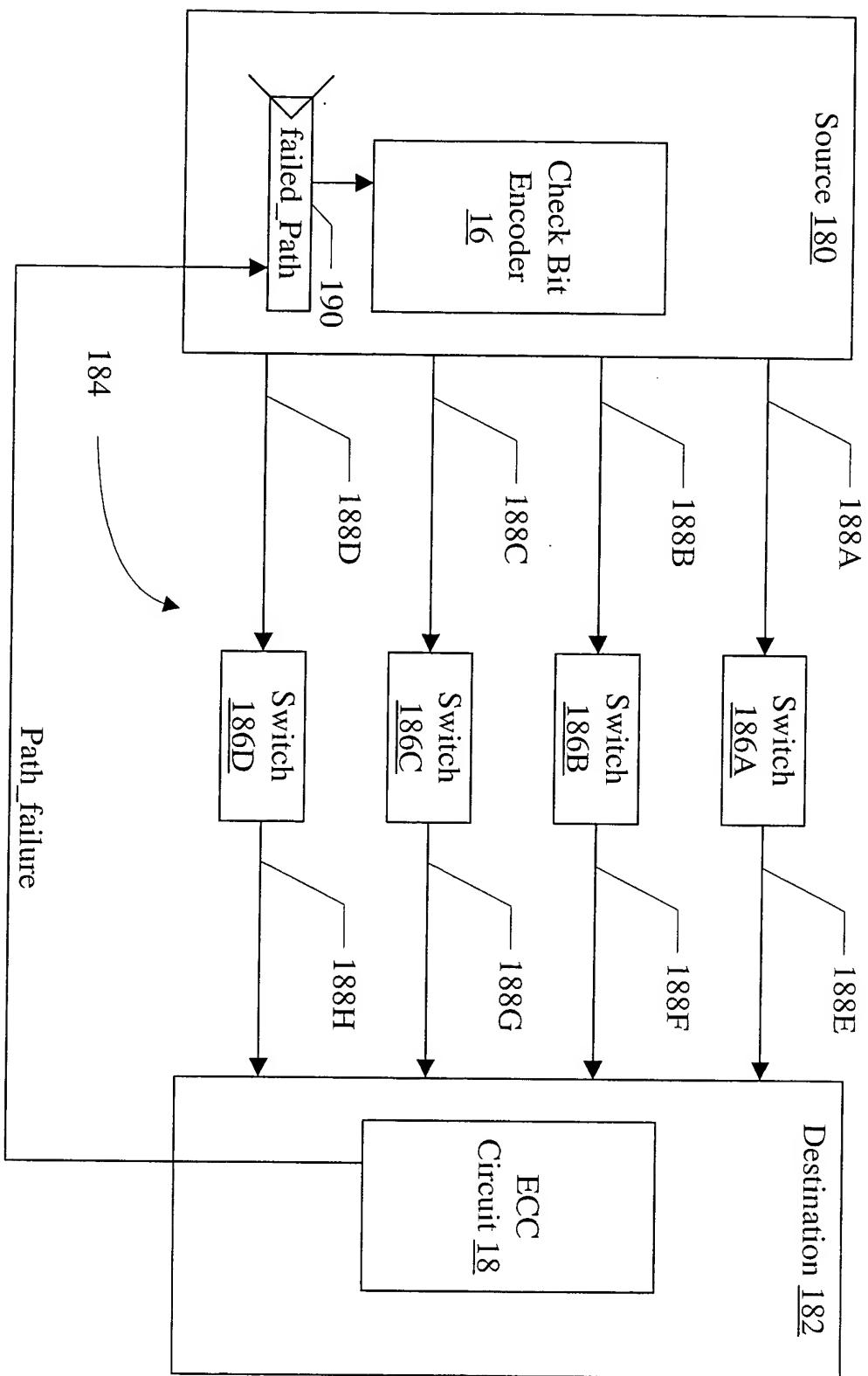


Fig. 10

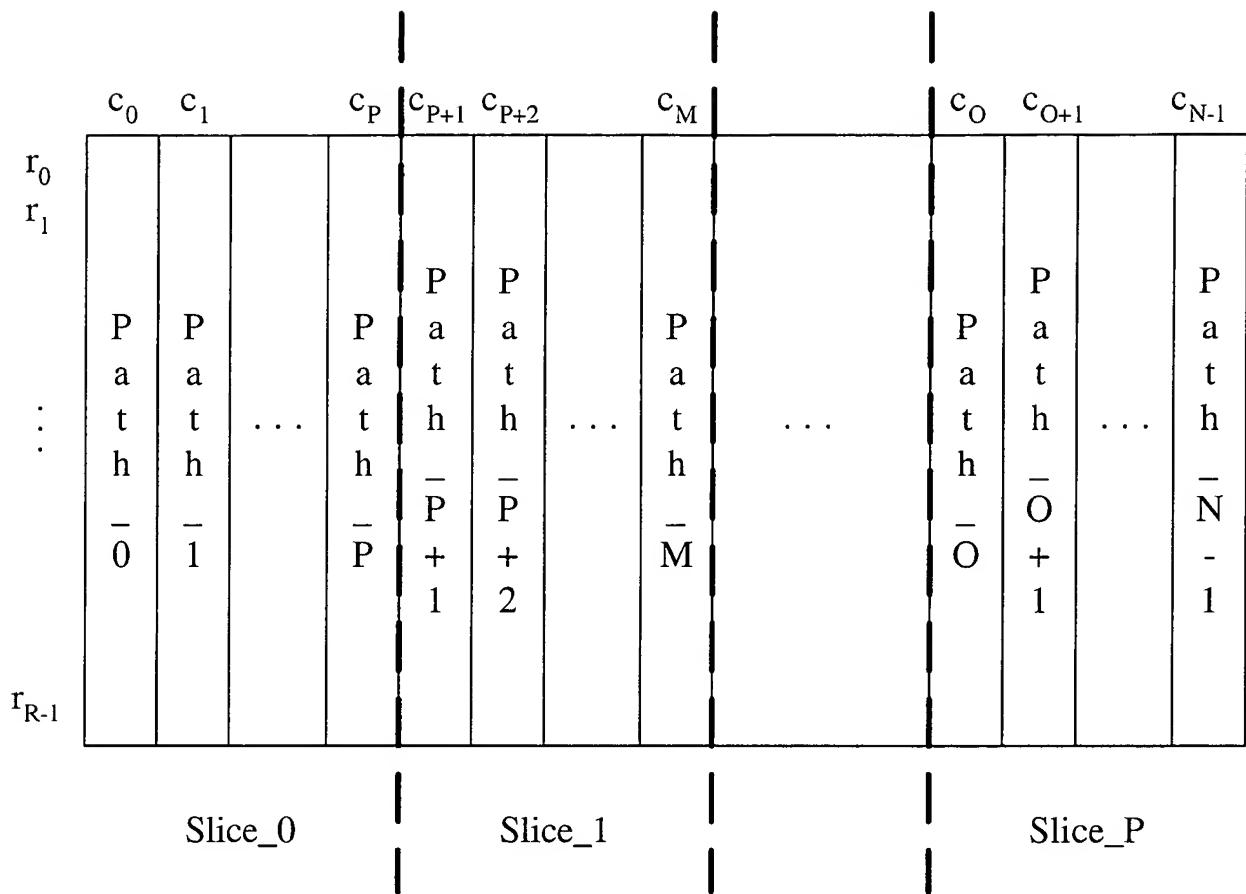


Fig. 11

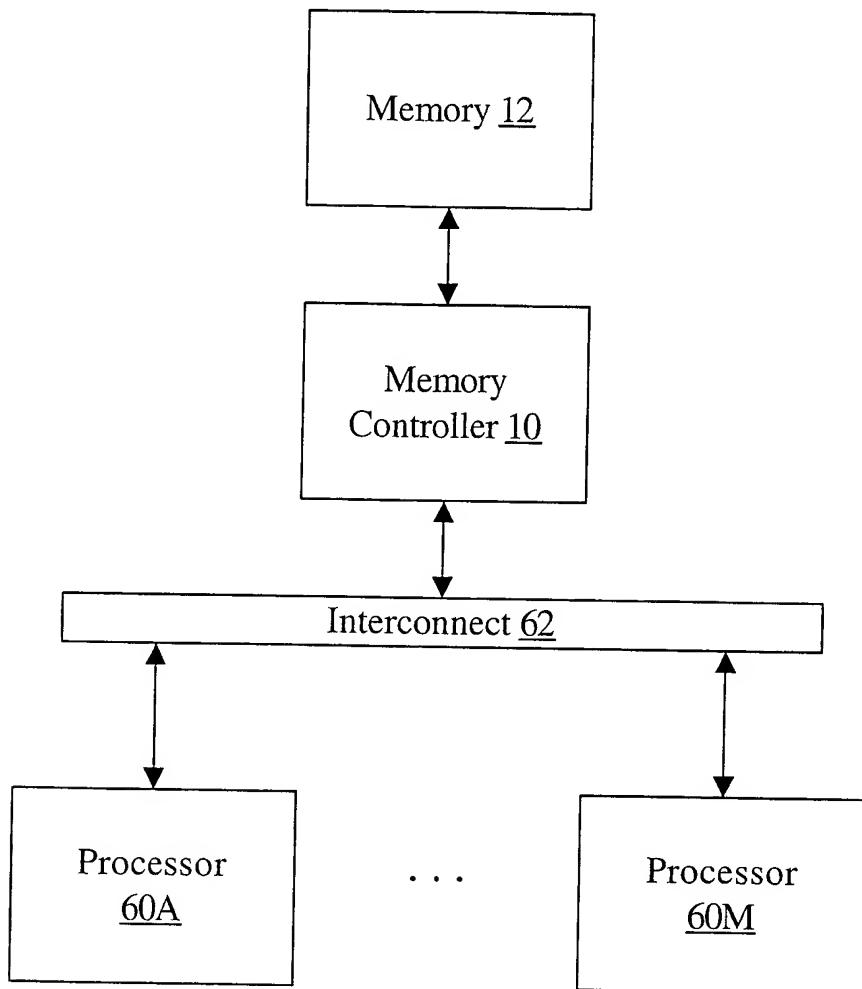


Fig. 12